



Important Security
Information for
System Administrators

DX8100 Digital Video Recorder

C2641M (9/06)

Contents

DX8100 Platform Security Information	6
Physical Security	6
Setting the BIOS Supervisor Password	6
Operating System Security	9
Windows Operating System Updates	9
Changing the Windows Administrator Password	10
Enabling Ctrl+Alt+Del	15
Using F2+F9+Del	15
Internet Protocol Security (IPSEC)	16
Viewing Video or Upgrading Client Software Over the Network	16
Background Color Configuration Security Issues	16
Antivirus Software and Virus Definitions Updates	17
Application Software	17
DX8100 Network Ports	18
Firewalls	18
Password Recovery	19
DX8100 System Recovery Procedure	20

List of Illustrations

1	DX8100 BIOS Setup Main Screen	7
2	New BIOS Password Dialog Box	7
3	Password Confirm Dialog Box	8
4	BIOS Setup Confirmation Screen	8
5	Users and Passwords Icon in Control Panel	10
6	Users and Passwords Dialog Box	10
7	Advanced Page	11
8	Users and Groups Dialog Box	11
9	User Listing Dialog Box	12
10	Enter and Confirm New Password	12
11	Set Password Dialog Box	13
12	Log On to Windows Dialog Box	13
13	Users and Passwords Dialog Box	13
14	User Name and Password Option Disabled	14
15	DX8100 IPSec Policy Dialog Box	16
16	Password Recovery Option in File Menu	19
17	Password Recovery Dialog Box	19
18	DX8100 BIOS Setup Main Screen	20
19	Boot Settings Page	21
20	Moving the CD/DVD Device to be First in List	21
21	Selecting OK to Save Changes	22
22	Warming Message and Recovery Configuration	22
23	IBIOS Setup Window	23
24	BIOS Boot Settings Page	23
25	Boot Device Priority Page	24
26	PDB Initialization Dialog Box	24
27	PDB Initialization Screen with Recovery Active	25
28	DX8100 System Page Date/Time Setup Area	25

List of Tables

A	DX8100 Keyboard Remapping	15
B	DX8100 Network Ports	18
C	Other Reserved Port Assignments	18

DX8100 Platform Security Information

The DX8100 Series digital video recorder (DVR) is equipped with an extensive set of security measures to assist in providing the user with secure, uninterrupted service.

NOTE: While great care has been taken in the design and development of the DX8100 to ensure a secure DVR platform, it is not feasible to protect a system from all internal and external security risks if it is connected to an unsecured network. In addition to the robust security features built into the DX8100, you should consult with your network administrator, information technology department, and facilities manager to ensure that all possible measures are being taken to ensure the safety and security of the DX8100 and its data.

The following sections describe the security features of the DX8100 in detail. These sections are intended for system administrators who are responsible for the maintenance and security of the DX8100.

PHYSICAL SECURITY

Like any other video recording device, including VCRs, the security of the DX8100 is largely dependent on the physical security of the unit itself. When an intruder has access to the hardware, it will be possible to remove components and retrieve recorded data. Units should therefore be installed in a location that is physically secured.

Because the dimensions and underlying technologies of the DX8100 are similar to those of a modern personal computer, it is possible to rack mount units and access the mouse and keyboard inputs using commercially available keyboard video mouse (KVM) switches. This may bring the control of the units outside of the secured area. One area where this could cause a problem involves access to the system's basic input/output system (BIOS). Pelco recommends that the unit be given a BIOS supervisor password upon completion of installation. A unique BIOS supervisor Password will help prevent remote operators from changing boot parameters that could allow the unit to be booted using unsecured sources.

The DX8100 is engineered to reboot automatically in the event of a system problem. The capability of recovering from certain errors without operator intervention minimizes the potential amount of time a DVR will be offline. To retain this capability, it is important that a password be set for BIOS Supervisor account only and not for the BIOS User account. Setting a password for the BIOS User account would force operators to re-enter this password each time the system is rebooted.

 **WARNING:** Always scan removable media, such as CD-RW and DVD-RW disks, for viruses before inserting them into the DX8100.

SETTING THE BIOS SUPERVISOR PASSWORD

The following procedure describes how to set the BIOS supervisor password. This procedure should be performed only by advanced users with extensive experience with PC computer technology. Changing BIOS settings to incorrect values may result in the degradation of system performance or cause your DVR to stop working.

To set the BIOS supervisor password:

1. Boot the DX8100 Series DVR by turning on the power switch.

2. Press the Delete key on the keyboard as soon as the Pelco splash screen is displayed. The BIOS Main screen appears.

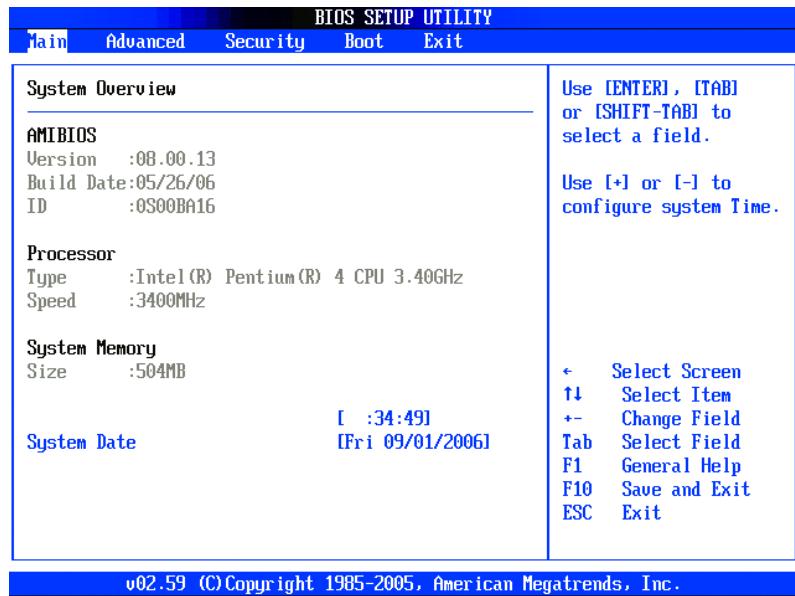


Figure 1. DX8100 BIOS Setup Main Screen

3. Use the cursor control keys on your keyboard to move over to the Security tab and select "Change Supervisor Password."
4. Press the Enter key on your keyboard. The Enter New Password dialog box opens.
5. Enter a new password for the BIOS Supervisor account. Passwords should be between four to six alphanumeric characters.
6. Press Enter key to accept the new password.

⚠ WARNING: Make sure that you only set the BIOS Supervisor Password. Do not assign a password to the BIOS User Password.

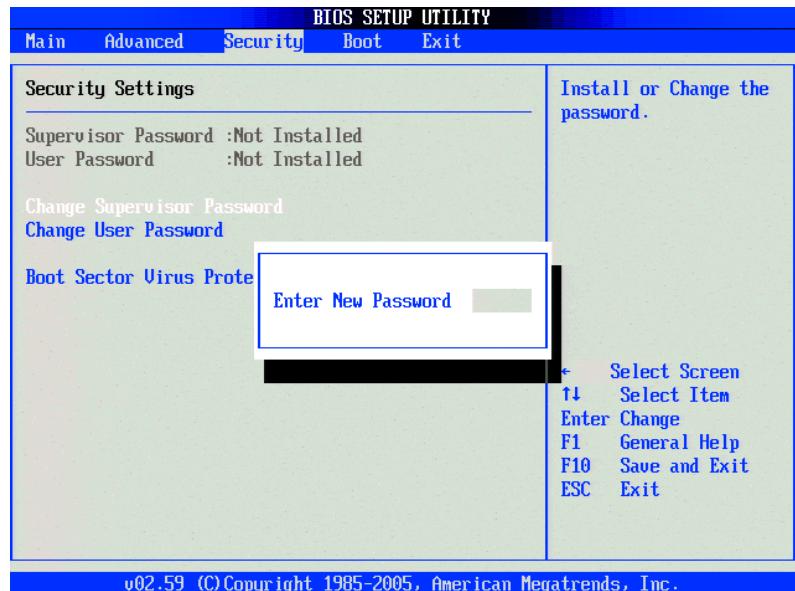


Figure 2. New BIOS Password Dialog Box

7. Re-enter the password again to confirm that it is correct.
8. Press the Enter key to confirm the new password.



Figure 3. Password Confirm Dialog Box

NOTE: Remember to write down this password and keep it in a secure place.

9. Press the F10 function key on your keyboard to save and exit the BIOS setup screen.

10. Finalize BIOS changes:

- To accept the BIOS changes and reboot, press the Enter key.
- To cancel the BIOS changes, press the Esc key and Ctrl+Alt+Delete to reboot the DX8100.

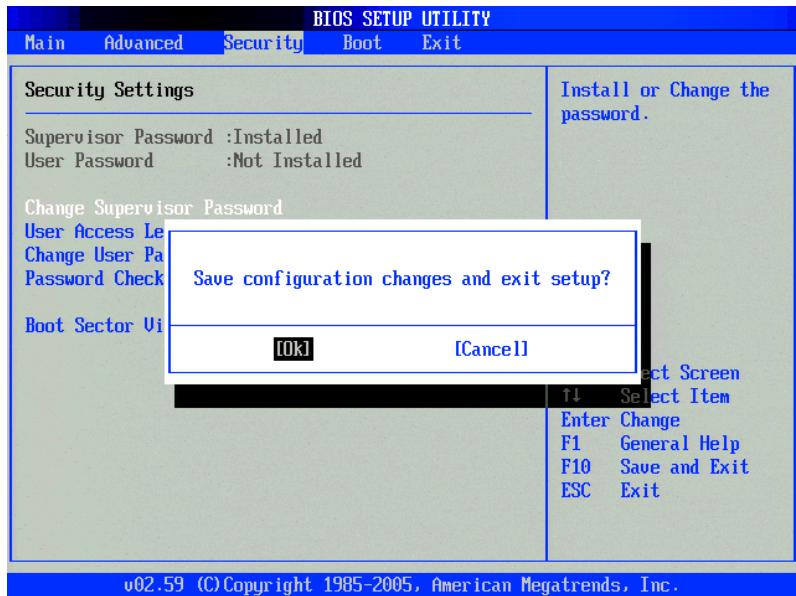


Figure 4. BIOS Setup Confirmation Screen

OPERATING SYSTEM SECURITY

Upon a successful boot procedure, the DX8100 will automatically load the Windows® 2000 operating system. This operating system is specifically tailored for use on the DX8100. It does not have the standard feature set found in the commercially available version of the Windows 2000 operating system. This means that services that are not needed for the correct operation of the DX8100 have been removed to eliminate potential vulnerabilities.

Only two user accounts are available in the DX8100's operating system software. These user accounts should not be confused with the accounts assigned by the DX8100 application software. An administrator account allows a designated user to make changes to the registry and security settings to accommodate the requirements of the specific site. A single user account, which is automatically logged in during boot up, is used to start and run the DX8100 application software. The capabilities of the user account have been dramatically reduced to prevent the default user from modifying the operating system setup.

This reduction of services and operating system capabilities is based on recommended lockdown procedures of the National Institute of Standards and Technology (NIST) for security-hardened computer systems. In addition to the NIST lockdown, a further lockdown of the Microsoft Internet Information Service (IIS) server has been implemented.

In finding a balance between security and functionality, Pelco has consistently opted for security but leaves it up to the administrator to unlock features that might be useful if the administrator has determined that the additional security of the lockdown is not needed. A typical example of this is the capability of the DX8100 to use dynamic IP addresses. Because IP addresses can change over time, clients must use a different mechanism to connect to the server than by simply providing an IP address. The additional use of NetBIOS protocol services allows the computer to find IP addresses on the local LAN by system name. However, the NetBIOS service also has a known vulnerability. To counter this vulnerability while still providing end users with a flexible platform, NetBIOS services are disabled at the factory but can be enabled by an administrator, when needed. The administrator then needs to apply alternative means to protect against hackers and viruses, for instance, by using a firewall. How to enable services on the DX8100 is outside the scope of this manual. Please check with your information technology specialist or contact Pelco Product Support for further instructions.

WINDOWS OPERATING SYSTEM UPDATES

Due to the lockdown of nonessential services on the DX8100, administrators are advised against installing every operating system upgrade published by Microsoft. The majority of these updates are not applicable to the DX8100. Pelco will redistribute any necessary operating system upgrades as part of a system upgrade.

CHANGING THE WINDOWS ADMINISTRATOR PASSWORD

This section describes how to change the Windows administrator password. The DX8100ADM password should be changed immediately upon installation of the DX8100 DVR. If the DX8100ADM account is not properly password protected, your system will be highly vulnerable to damage and improper use from a variety of security threats.

Before attempting to access or change the DX8100ADM account, be aware that only authorized personnel with advanced technical experience working with the Windows 2000 operating system should log into or change the DX8100ADM account. Damage to the DX8100, its system and application software, and loss of critical data may result from improper use of the DX8100ADM account. You must have the Windows password to exit from the DX8100 application to the Windows operating system. The Windows default password is "dx8100."

To change the Windows 2000 DX8100ADM password:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Click Start > Settings > Control Panel. The Windows Control Panel appears.

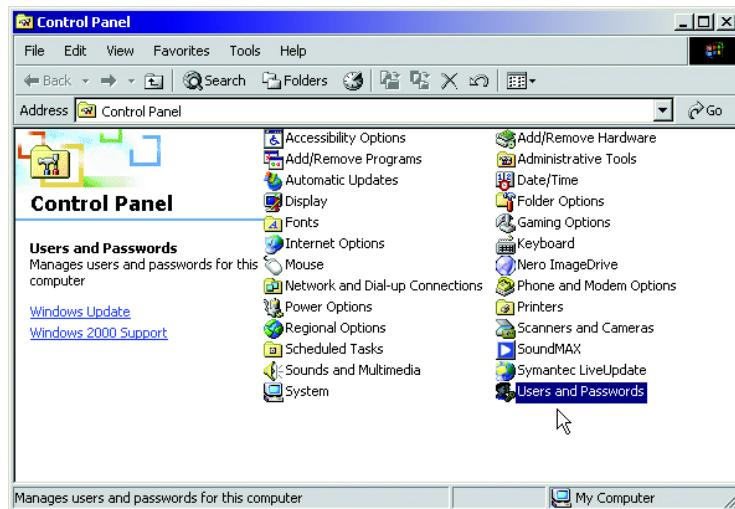


Figure 5. Users and Passwords Icon in Control Panel

3. Double-click the Users and Passwords icon. The User and Passwords dialog box appears.

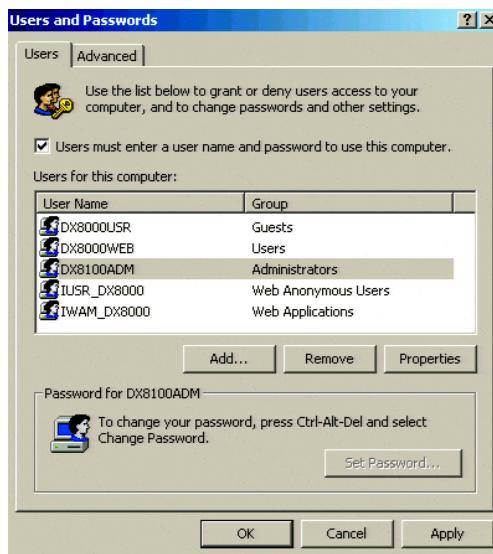


Figure 6. Users and Passwords Dialog Box

4. Click the Advanced tab. The Advanced page appears.



Figure 7. Advanced Page

5. Click the Advanced button. The Local Users and Groups dialog box appears.

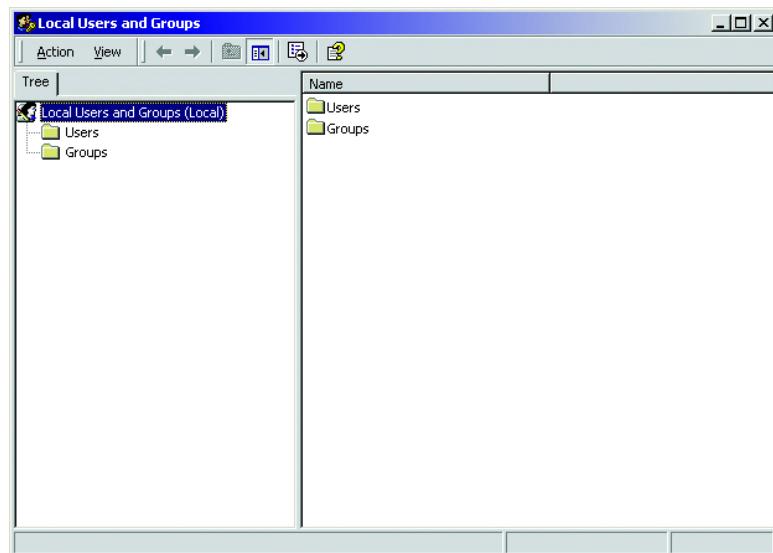


Figure 8. Users and Groups Dialog Box

6. Click Users.

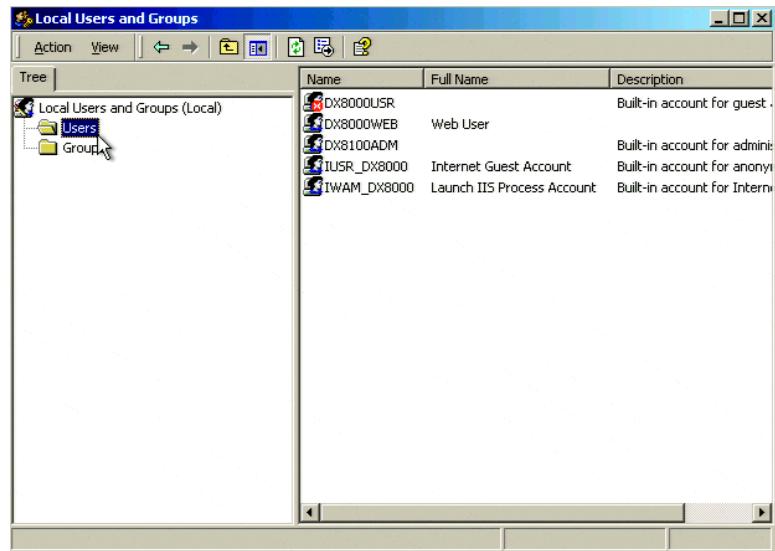


Figure 9. User Listing Dialog Box

7. Right-click DX8100ADM and then select the Set Password option from the shortcut menu.

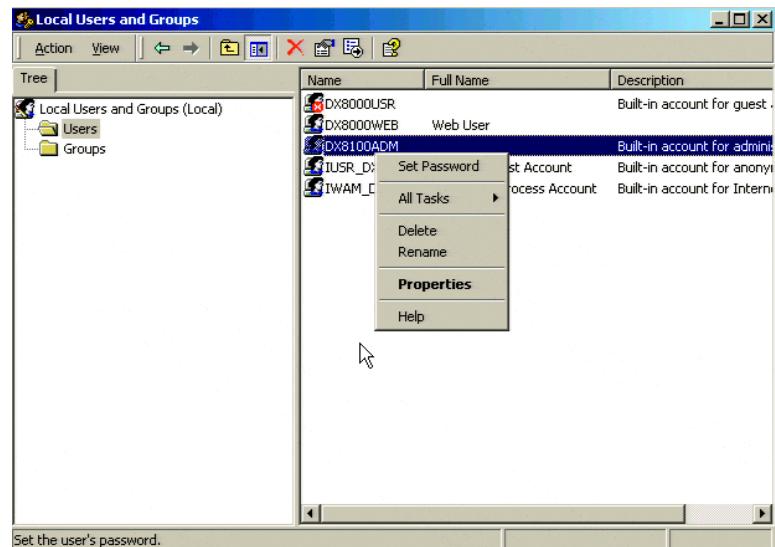


Figure 10. Enter and Confirm New Password

The Set Password dialog box appears.

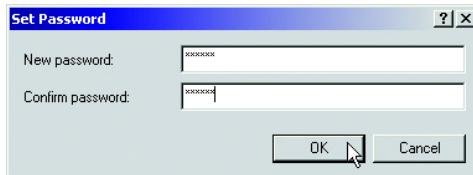


Figure 11. Set Password Dialog Box

8. Enter a new password for the DX8100ADM account. Passwords are case-sensitive and should contain a mixture of alphabetic and numeric characters between six and ten characters in length.

NOTE: Remember or write down this password and keep it in a secure place.

9. Click OK. The Set Password dialog box closes.
10. Close the Local Users and Groups dialog box and click OK.
11. Click Start > Shutdown > Restart to reboot the DX8100. The Log On to Windows Dialog Box opens.



Figure 12. Log On to Windows Dialog Box

12. Enter the new password and click OK. The DX8100 server application opens.

To enable the automatic logon feature:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Click Start > Settings > Control Panel. The Control Panel dialog box opens.
3. Double-click Users and Passwords icon. The Users and Passwords dialog box opens.

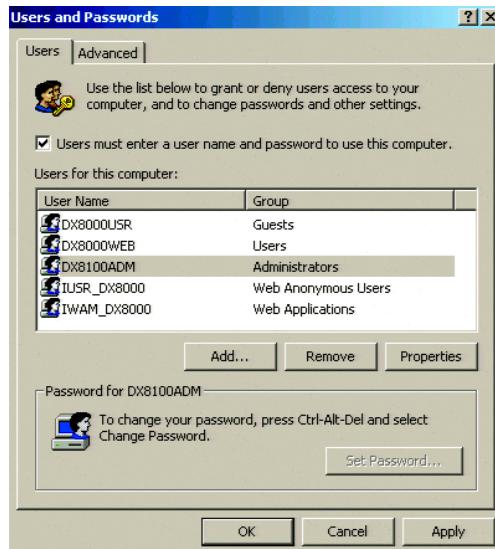


Figure 13. Users and Passwords Dialog Box

4. If the “Users” tab is not selected, click the Users tab.
5. In the “Users for this computer” area, select “DX8100ADM.”
6. If “Users must enter a user name and password to use this computer” check box is selected, deselect the check box to enable the automatic logon feature.

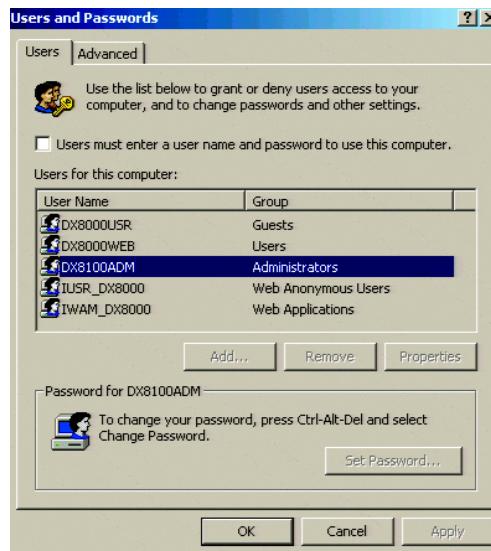


Figure 14. User Name and Password Option Disabled

7. Click OK.

ENABLING CTRL+ALT+DEL

Enabling the Ctrl+Alt+Del key combination allows you to open the Windows Task Manager dialog box to perform Windows system administration tasks. To complete the procedure, you must be logged on to the DX8100 as an administrator or a member of the administrators group on a computer that is part of a network domain.

The standard Ctrl and Alt keys are remapped for the DX8100 application. Table A describes how the DX8100 keyboard is remapped.

Table A. DX8100 Keyboard Remapping

DX8100 Key	Windows Action
F2	Ctrl
F4	Space
F9	Alt
Ctrl	Space
Alt	Space

The key combination used to implement Ctrl+Alt+Del is F2+F9+Del.

To enable the Ctrl+Alt+Del key feature:

1. Click .
2. Click .
3. From the Setup Ctrl + Alt + Del key combination area, click the Enable Ctrl+Alt+Del key combination selection check box.
4. Click Apply.
5. Reboot the DX8100.

USING F2+F9+DEL

The Ctrl+Alt+Del feature must first be enabled. F2+F9+Del allows you to access the Windows Task Manager dialog box from within the DX8100 shell. When you exit the Windows environment, you are returned to the DX8100 shell. In this case, you do not have to log back into the DX8100.

To access the Windows Task Manager dialog box:

1. Press F2+F9+Del. The Windows Security dialog box opens.
2. In the Windows Security dialog box, click Task Manager. The Windows Task Manager window opens.
3. To return to the DX8100 shell without rebooting the DX8100, exit the Windows Task Manager dialog box.

INTERNET PROTOCOL SECURITY (IPSEC)

The DX8100 features built-in network security using IPSec. IPSec facilitates authentication and encryption at the network packet level. IPSec security services protect the DX8100 from unwanted or potentially damaging network requests. With IPSec enabled, the DX8100 DVR will not respond to any unsecured communication across the network, whether friendly or malicious. IPSec only blocks unwanted or unauthorized communication flowing to the DX8100. It does not hinder communication sessions that are initiated by the DVR. IPSec security is enabled by default on the DX8100; however a system administrator can disable the service if it is deemed necessary for the proper functioning of the unit.

⚠ WARNING: Disabling IPSec security services will expose your DX8100 Series DVR to potentially damaging network traffic. It is highly recommended that IPSec security is enabled at all times for the protection of your system.

To disable IPSec security services on the DX8100 Series DVR:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Go to Start > Programs > Manage IPSec Policy. The DX8100 IPSec Policy dialog box appears.



Figure 15. DX8100 IPSec Policy Dialog Box

3. Deselect the Enable DX8100 IPSec Policy check box. Reselect the Enable DX8100 IPSec Policy check box to re-enable IPSec security.
4. Click OK.

VIEWING VIDEO OR UPGRADING CLIENT SOFTWARE OVER THE NETWORK

If you encounter a problem viewing video or upgrading your PC Client software over the network from a DX8100 sever, try turning off IPSec on both the DX8100 server and PC Client machine.

If that produces video, leave IPSec turned off. Be advised that disabling IPSec security services will expose your DX8100 Series DVR to potentially damaging network traffic. For more information on protecting your system from harmful network traffic, contact your network administrator.

If only the PC Client update is affected, turn IPSec back on after the application is updated. It is highly recommended that IPSec security be enabled at all times for the protection of your system.

BACKGROUND COLOR CONFIGURATION SECURITY ISSUES

The DX8100 server software allows a guest user to set the background color displayed underneath the text. However, the background color feature allows the guest user to gain access to the Windows environment through a back door in the Background Color dialog box.

After opening the Set Color dialog box, the guest user can access the Windows environment as follows:

1. In Set Color dialog box, click Custom Colors. The Windows Color dialog box opens.
2. Right click on a color. The Windows What's This submenu is displayed.
3. Click What's This. The tool tip message is displayed.
4. Right click the tool tip. A submenu is displayed giving the guest user the option to copy or print the tool tip topic.
5. Click Print Topic. The Windows Print wizard opens, which eventually allows the guest user to gain access to the Windows environment.

In this case, if a printer is not configured for the system, the guest user is denied further access to the Windows environment. But it is likely that most DX8100 servers installed in the field have printers attached to them. If a printer is not attached, the guest user can set up a dummy printer.

The work-around for the above-described security breach is to block or further lock down the Custom Colors feature by disabling the What's This option for all users.

ANTIVIRUS SOFTWARE AND VIRUS DEFINITIONS UPDATES

The DX8100 supports Symantec AntiVirus® Corporate Edition 9.0 and McAfee VirusScan Professional Edition 8.0 antivirus software. To provide an additional degree of protection against viruses, either of one of these antivirus programs can be installed, configured, and activated on each DX8100 DVR in your organization.

For more information about supported antivirus software, refer to the latest version of following documentation:

- For Symantec AntiVirus Corporate Edition 9.0, go to URL <ftp://www.pelco.com/ProductManuals/C1613M.PDF> to see Using Symantec AntiVirus Corporate Edition Version 9.0 Software On a DX8100 DVR.
- For McAfee VirusScan Professional Edition 8.0, go to URL <ftp://www.pelco.com/ProductManuals/C1611MA.PDF> to see Using McAfee VirusScan Professional Edition Version 8.0 Software On a DX8100 DVR.

NOTE: New viruses are created every day. To remain effective, your antivirus software must be active and updated on a regular basis. Pelco is not responsible for the failure of an individual or organization to update antivirus software and virus definition files. Scanning the hard disk system for viruses while the DX8100 is recording may result in lost video data. Virus scanning should only be performed manually while the DX8100 is not in record, search, or playback modes. Pelco is not responsible for damage or loss to equipment, software, video, or other data resulting from computer viruses. Please refer to your antivirus software manual for more information on protecting against the viruses.

APPLICATION SOFTWARE

The only application intended and guaranteed to work on the DX8100 unit is the DX8100 application software itself. Do not install other application software. If you do, this voids the warranty on the unit, and it also opens up potential holes in the system security. The DX8100 application software has several user and group accounts with varying degrees of rights and permissions on the system. Each account is password-protected. These accounts and passwords are completely different from the operating level account and password discussed in the previous section. The typical system operator will have to work only with application program level user names and passwords.

DX8100 NETWORK PORTS

Table B describes the DX8100 default ports and their function. The DX8100 ports are classified either as user-changeable or fixed. You can assign a user-changeable port a different number. In this case, a user-changeable port's number must be assigned within the range of 5000 to 6535. If a port is assigned out of this range, the system displays a message alerting you that an invalid port number is being used. You cannot assign a different number to a fixed port.

Table B. DX8100 Network Ports

Port Number	User-Changeable	Function
9002	Yes	DX8100 base port: Used for transmission of video, audio, and interface data
9003	Yes	Software upgrade port: Used for remote upgrade of DX8100 software
9004	Yes	Agent port: Used for emergency agent notification
9005	No	Information port
13900	No	Ping port

NOTE: Unless there is a conflict on your network, it is recommended that you do not change port numbers from their default settings. Make sure any changes to port numbers are made consistently across all DX8100 servers and clients on a network. Client and server ports must be identical.

The DX8100 port functionality is summarized as follows:

- Base port: This port is configured at the DX8100 Network setup screen. The base port number is downloaded to the PC client system during an IP scan. The port number can be modified at the DX8100 Site Setup screen.
- Software Upgrade Port: This port is configured at the DX8100 Network setup screen. The upgrade port number is downloaded to the PC client system during an IP scan. The port number can be modified at the DX8100 Site Setup screen. The PC client's upgrade port number must match the DX8100 server's upgrade port number. For server-to-server software upgrades, both server software upgrade port numbers must match.
- Agent Port: This port is configured at the DX8100 Notification setup screen. You change the client emergency agent server listening port using the Emergency Agent application running on the PC client system. For more information about changing the client emergency agent listen port, see the Client Applications manual.

Table C lists other reserved port information.

Table C. Other Reserved Port Assignments

Port Number	Description
0	Not used
1–255	Reserved for well-known services at network communication
256–1023	Other reserved ports
1024–4999	Temporal client ports (OS allocates automatically)
5000–6535	User-defined ports

FIREWALLS

Firewalls are used to keep external systems from exploiting vulnerabilities in the operating system that are linked to the Windows TCP/IP socket system. Regardless of which port or service is under attack, the port must be open or at least visible in order for the malicious program to exploit it. Firewalls render all ports that are not needed invisible and hence form an excellent protection against such attacks. Networked systems exposed in anyway to the outside world (such as when connected to the Internet) should be equipped with a firewall.

PASSWORD RECOVERY

There are no "backdoor" accounts or alternative access options built into the DX8100 application software. Pelco cannot issue overriding passwords, factory passwords, or other means to bypass the log-in requirement of the application program. If the DX8100's Admin account password is lost or forgotten, there is only one method for resetting the Admin password without completely reinstalling the system from the Recovery CD.

Upon request, Pelco can issue a unique password recovery code that is valid for 24 hours only. The recovery code is exclusive to the machine for which it is issued. If needed, the original buyer of the system (typically the dealer) may contact Pelco Technical Support with the serial number and order or invoice number on which the unit was originally purchased. This must be done in writing, and the request must be accompanied by a letter from the current owner of the system stating the he or she is the legal owner of the system, the password for the system was lost, the MAC address for the DVR(s) for which a reset code is needed, and that he or she is requesting a password reset code. Upon verification, Pelco will issue a reset code that can be used for 24 hours on the DX8100 with the provided MAC address only.

To recover a lost or forgotten Admin password:

1. Go to File > Password Recovery. The Password recovery dialog box opens.



Figure 16. Password Recovery Option in File Menu

2. Contact Pelco Product Support with the following information:
 - a. MAC address as it appears in the Password Recovery dialog box.
 - b. Current date for your location as it appears in the Password Recovery dialog box.
 - c. Any additional information requested by Pelco Product Support

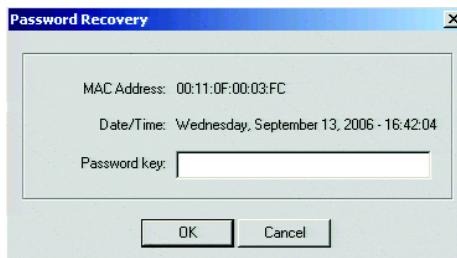


Figure 17. Password Recovery Dialog Box

3. Enter the new password you obtained from Pelco Product Support in the field provided.
4. Click OK.

DX8100 SYSTEM RECOVERY PROCEDURE

This DX8100 recovery procedure is used in two ways:

- To recover your DX8100 software using the DX8100 Recovery DVD that is provided with the DX8100.
- To recover your DX8100 Series DVR in case of a catastrophic failure. In this case, this procedure should only be thought of as a last resort endeavor. The recovery process erases the entire contents of your DVR's primary hard disk drive and overwrites the disk with a fresh image of the system and application software from the DX8100 Recovery DVD.

To reinitialize your DX8100 Series DVR and reinstall all operating system and application software:

1. Insert the DX8100 Recovery DVD into the DVD drive.
2. Do the following:
 - a. Restart the DX8100.
 - b. Enter the BIOS by pressing Delete at the point the Pelco splash screen is displayed. The BIOS Setup UTILITY opens.

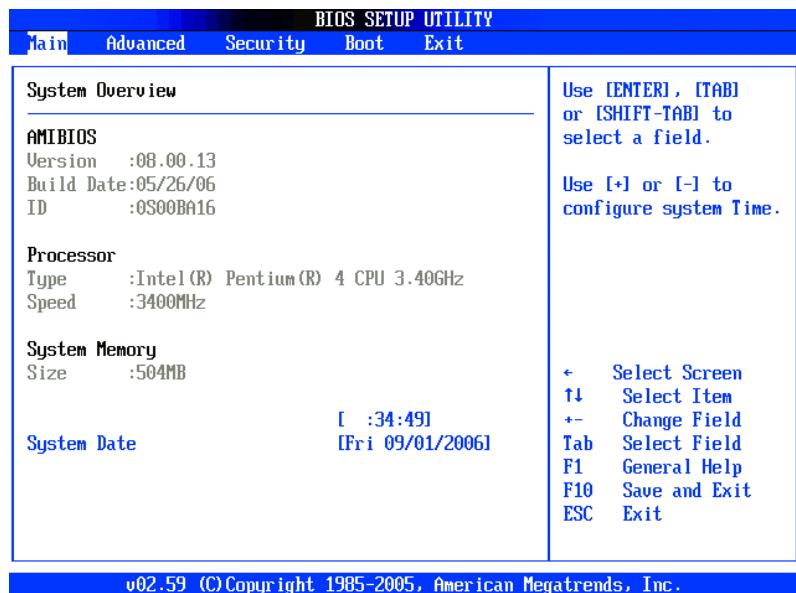


Figure 18. DX8100 BIOS Setup Main Screen

- c. In the BIOS setup, go to the Boot tab, select Boot Device Priority, and then press Enter. The Boot Settings page is displayed.

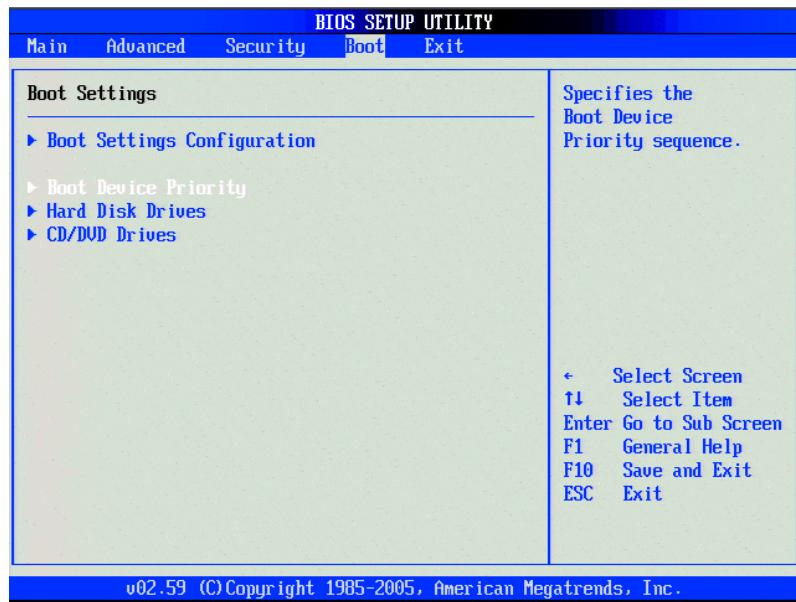


Figure 19. Boot Settings Page

- d. In the Boot Settings page, select Boot Devices Priority. and press Enter. The Boot Device Priority page is displayed.
- e. In the Boot Device Priority page, press the keyboard \pm key until CD/DVD is #1 in the list.

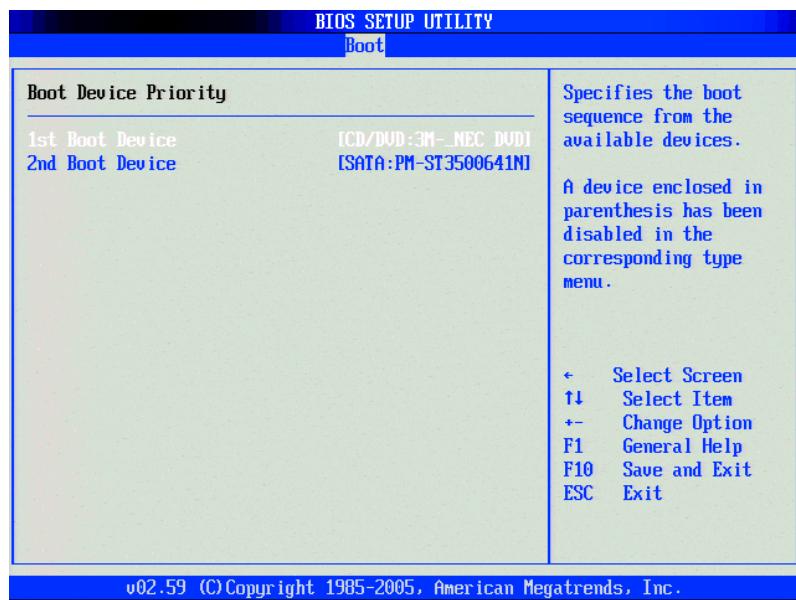


Figure 20. Moving the CD/DVD Device to be First in List

f. Press F10 and then select OK to save your changes and exit. The DX8100 will restart and prompt you by displaying "Press any key to boot from CD."

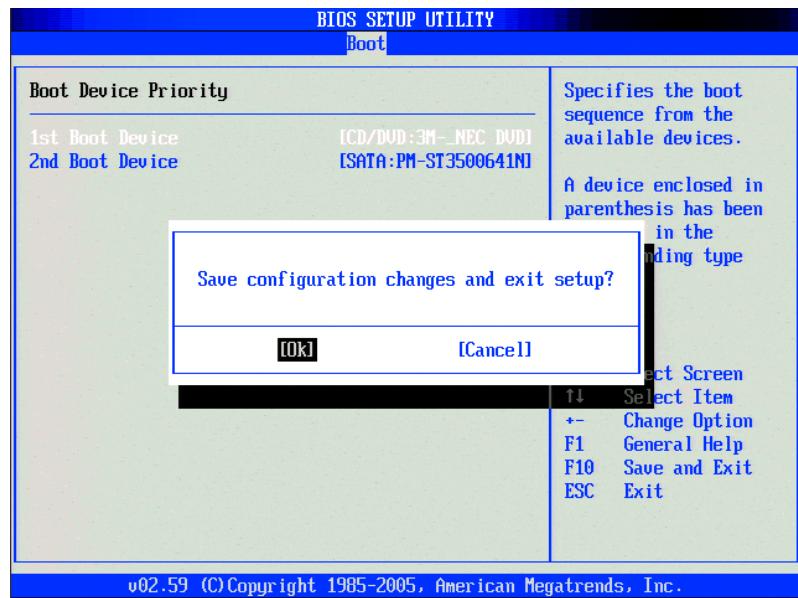


Figure 21. Selecting OK to Save Changes

NOTE: The prompt "Press any key to boot from CD/DVD is displayed for only a few seconds and if missed the unit will not boot from the DX8100 Recovery DVD.

g. Press the Space bar. After the DVD finishes loading, the Warning screen is displayed.
 h. Type **Yes** in the text box to agree to the recovery procedure, and then click Proceed.
 i. Click Exit after the clone process is completed to restart the DX8100. The DX8100 restarts.

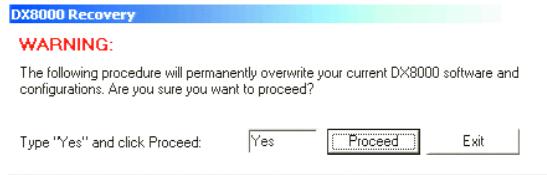
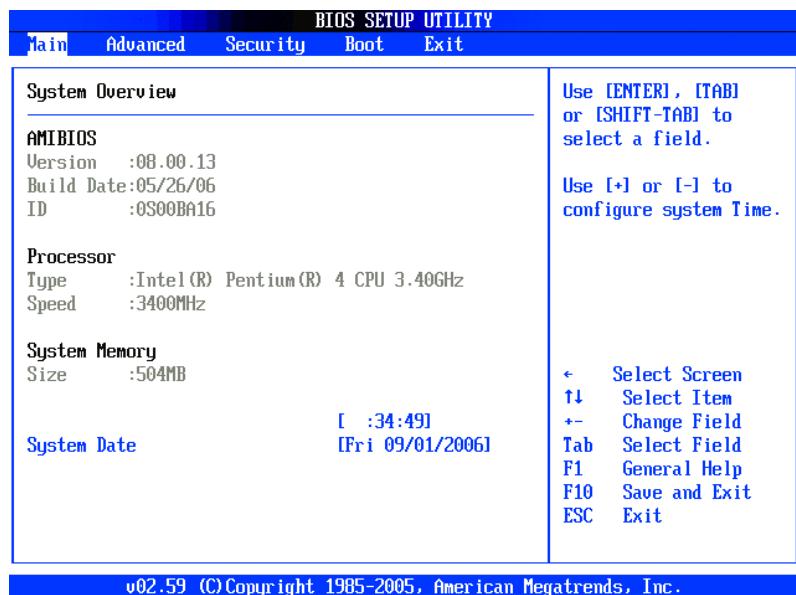


Figure 22. Warming Message and Recovery Configuration

3. Do the following:

- Enter the BIOS by pressing Delete at the point the Pelco splash screen is displayed. The BIOS Setup UTILITY opens.



v02.59 (C) Copyright 1985-2005, American Megatrends, Inc.

Figure 23. IBIOS Setup Window

- In the BIOS setup, go to the Boot tab, select Boot Device Priority, and then press Enter. The Boot Settings page is displayed.



v02.59 (C) Copyright 1985-2005, American Megatrends, Inc.

Figure 24. BIOS Boot Settings Page

- c. In the Boot Settings page, select Boot Devices Priority. and press Enter. The Boot Device Priority page is displayed.
- d. In the Boot Device Priority page, select SATA, and press \pm until SATA is #1 in the list.

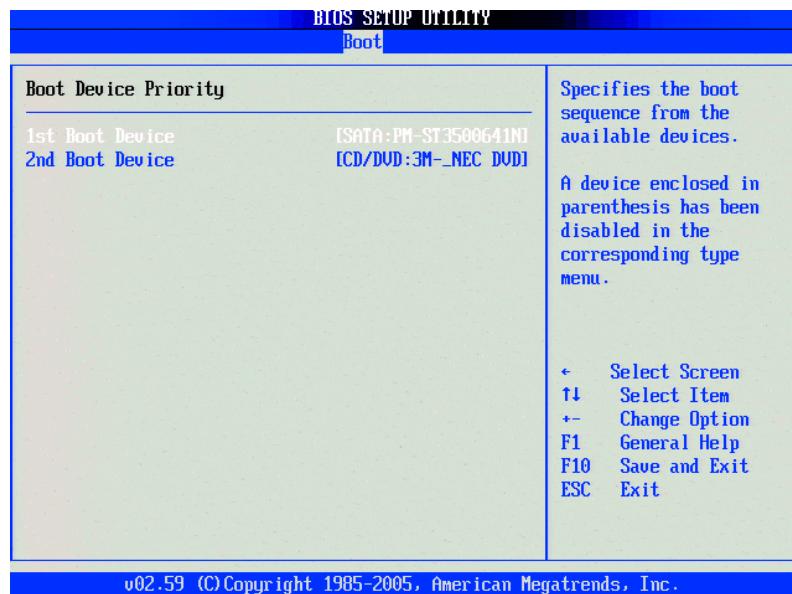


Figure 25. Boot Device Priority Page

4. Eject the DX8100 Recovery DVD.
5. Press F10 and then select OK to save changes and exit. The DX8100 will reboot and prompt you to initialize the hard disks for use with the DX8100 database.
6. Click "+" next to the PDB Group ID box to expand the tree.

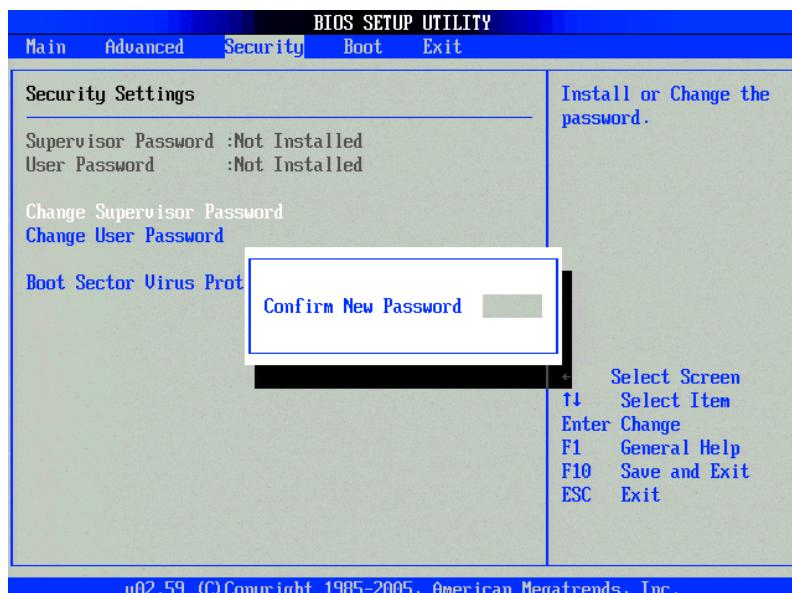


Figure 26. PDB Initialization Dialog Box

- If you are updating an existing system and you want to save previously recorded video, select Recovery on the PDB Group ID box. In this case, “all of the boxes should turn yellow and the individual drives should have Used selected.” This step will save your recorded video.

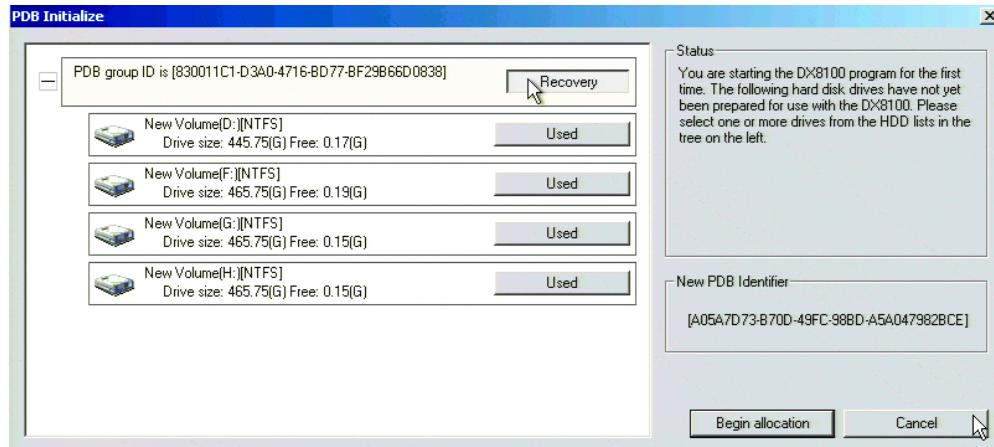


Figure 27. PDB Initialization Screen with Recovery Active

- If you are installing this system for the first time, make sure that Allocation is selected on each of the individual disk drives in the tree. This step will erase all data on all of the drives.

7. Click Begin Allocation to start the database initialization. Depending on the drive configuration, the DX8100 will take about 5 to 15 minutes to initialize the database and begin operation.
8. **(IMPORTANT)** Immediately after the DX8100 completes initializing the database, in the Date/Time Setup area of the System Setup page, verify that the DX8100 date, time, and time zone settings are correct.



Figure 28. DX8100 System Page Date/Time Setup Area

 **Green** The materials used in the manufacture of this document and its components are compliant to the requirements of Directive 2002/95/EC.

REVISION HISTORY

Manual #	Date	Comments
C2641M	9/06	Original manual.

Pelco, and the Pelco logo are registered trademarks of Pelco.
Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.
AntiVirus is a trade mark of Symantec Corporation.
VirusScan is a registered trademark of Network Associates, Inc.

©Copyright 2006, Pelco. All rights reserved.



Worldwide Headquarters
3500 Pelco Way
Clovis, California 93612 USA

USA & Canada
Tel: 800/289-9100
Fax: 800/289-9150

International
Tel: 1-559/292-1981
Fax: 1-559/348-1120

www.pelco.com

ISO9001